SOSCON

Improving 5G security and Open Source environment with ONAP penetration testing

Samsung R&D Institute Poland | Open Source Group | Krzysztof Opasiak

Agenda

What is ONAP?

Why we test ONAP security?

Pentest results

Influence on the community

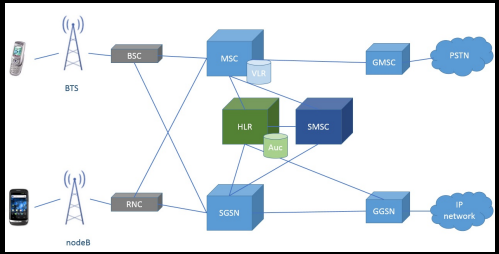
Summary

SOSCON

What is ONAP?

Traditional Network

- Black-box
- Specific hardware
- Proprietary vendor solution
- Interoperability issues
- Statically composed

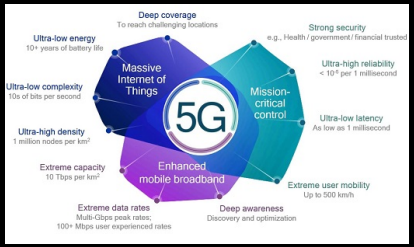


Source: realtimecommunication.wordpress.com

What is 5G?

- Enhanced Mobile Broadband
- Massive IoT
- Mission-critical control

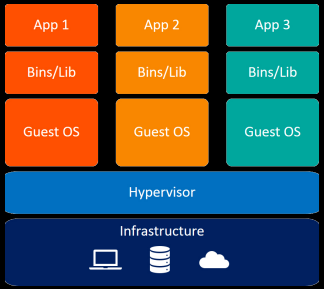
- Software Defined
- Cloud
- Edge



Source: researchgate.net

Virtual Network

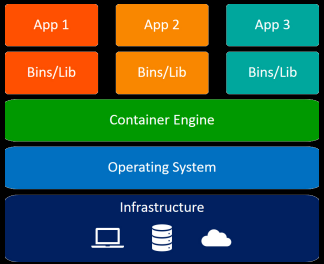
- Universal HW
- Virtual Network Functions
- Better scalability
- Better interoperability



Source: bmc.com

Containerized Network

- Platform instead of HW
- Micro-service architecture
- Extreme modularity
- Fine-grained scalability



Source: bmc.com

How to manage that?

- Composition
- Placement
- Connection
- Monitoring
- Scaling

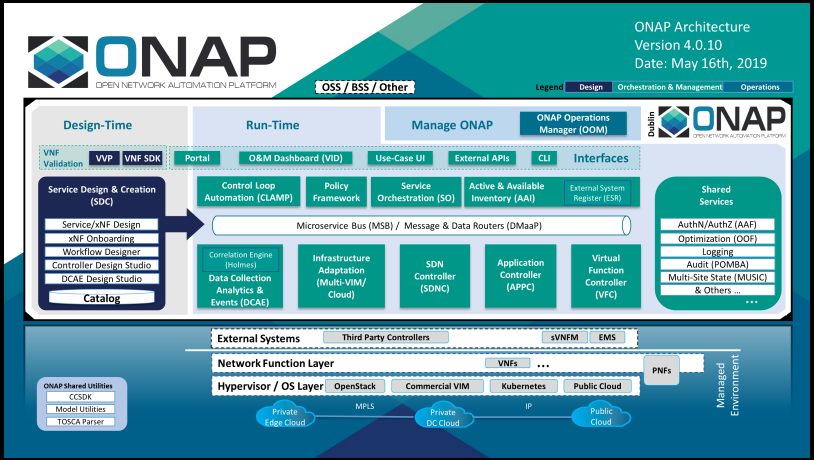
How to manage that?

- Composition
- Placement
- Connection
- Monitoring
- Scaling

Source: sampi.co

Scale is an issue!

ONAP



Source: wiki.onap.org

SOSCON

Why we test ONAP security?

5G security concerns

- Privacy
- Running external payloads
- Dynamic reconfigurability

Why ONAP security matters?

- ONAP manages whole network
- It Has a full access to the HW and SW
- It can do almost anything with the network

Source: marketwatch.com

Identified attack vectors

- Malicious Insider
- Worms
- Malicious payloads
- Tampered infrastructure

Source: nakedsecurity.sophos.com

Assumptions

- Secure deployment
- No OS-level vulnerabilities
- Properly configured kubernetes cluster
- Access to all services exposed outside of K8s cluster

Goals

- Asses overall ONAP security
- Find different types of vulnerabilities
- Report all findings back to the community
- Minimize commercialization cost

SOSCON

Pentest results

Network-related vulnerabilities

- Huge exposure (over 100 ports)
- Plain text protocols used
- Lack of SSO and RBAC
- Debugging tools (jolokia, RDWP) exposed
- API documentation exposed

Code-related vulnerabilities

- **SQL Injections**
- **XSS**
- **Crypto-related errors exposed to the user**

Deployment-related vulnerabilities

- Number of services run as a root
- Stack traces enabled and returned to the user
- The same passwords reused for all deployments

Other issues

- Security release notes were not helpful at all
- Lack of documentation on current state of ONAP
- Lack of ONAP security guideline

SOSCON

Influence on the community

Direct influence

- 28 CVEs assigned
- almost 200 Security tickets created
- Revised Vulnerability Management Process
- Focus community on production readiness

Raised security awareness

- Regular security-related discussion
- Requirements are not enough
- Projects started fixing security issues

El Alto release

- El Alto was a shorter release
- No new functionality
- Dedicated to reduce technical debt
- Especially security fixes

SOSCON

Summary

Future Work

- Security is not a one time task
- Pentest should be repeated in next year
- Security regression tests should be developed

Summary

- ONAP is going to be a key component of 5G network
- Its security is extremely important
- Early pentest has a lot of benefits
- Collaboration with the community allows to share the cost of fixing security issues

Thank you!

Krzysztof Opasiak

Samsung R&D Institute Poland

+48 605 125 174
k.opasiak@samsung.com